



PATENT APPLICATION
ATTORNEY DOCKET: 10624.0015

Trade Application of:

MARCEL M. YUNG ET AL

Serial No.: 09/429,624

Filed: October 29, 1999

For: INCORPORATING SHARED
RANDOMNESS INTO DISTRIBUTED
CRYPTOGRAPHY

Group Art Unit: 2766

Examiner: C. Tucker

Date: April 2, 2001

#8/
A

TS#
4-18-01

only
Claims
Added

RECEIVED
APR -9 2001
TC 2100 MAILROOM

RESPONSE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This is a reply to the Office communication dated October 3, 2000 ("the pending Action") in the above-identified application ("the pending Application").

AMENDMENTS

Please amend the pending Application as follows.

IN THE CLAIMS:

Please amend the following claims as set forth below:

- (N.E.)
Mark up
Copy not
included.
1. A method of distributed cryptographic computation using a plurality of distributed electronic devices, said method comprising:
 - (a) computing shared values over a known and agreed context;
 - (b) generating random values using said shared values;